FIG.1

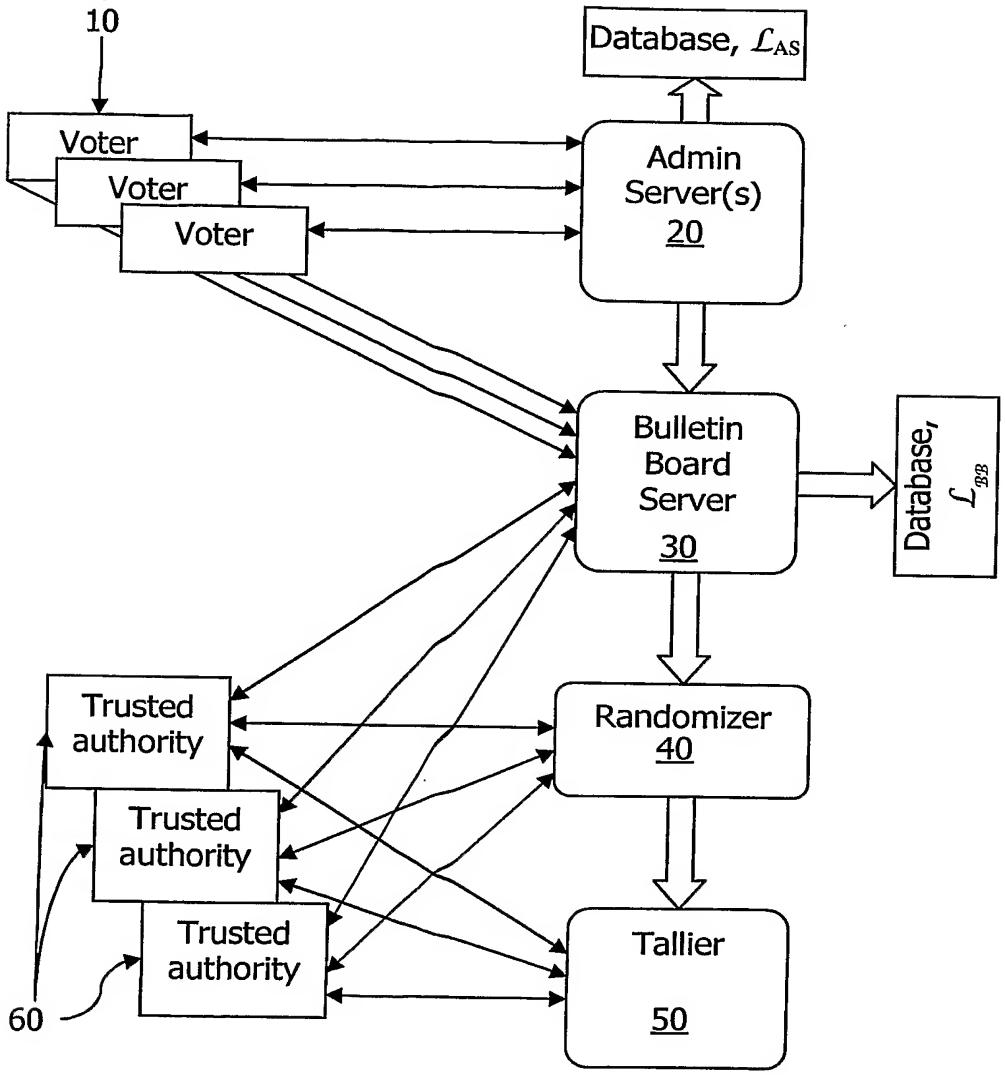

10
Database, $\mathcal{L}_{AS}$
Voter
Voter
Voter
Admin Server(s) 20
Bulletin Board Server 30
Database, $\mathcal{L}_{BB}$
Trusted authority
Trusted authority
Trusted authority
Randomizer 40
Tallier 50
60

FIG.2

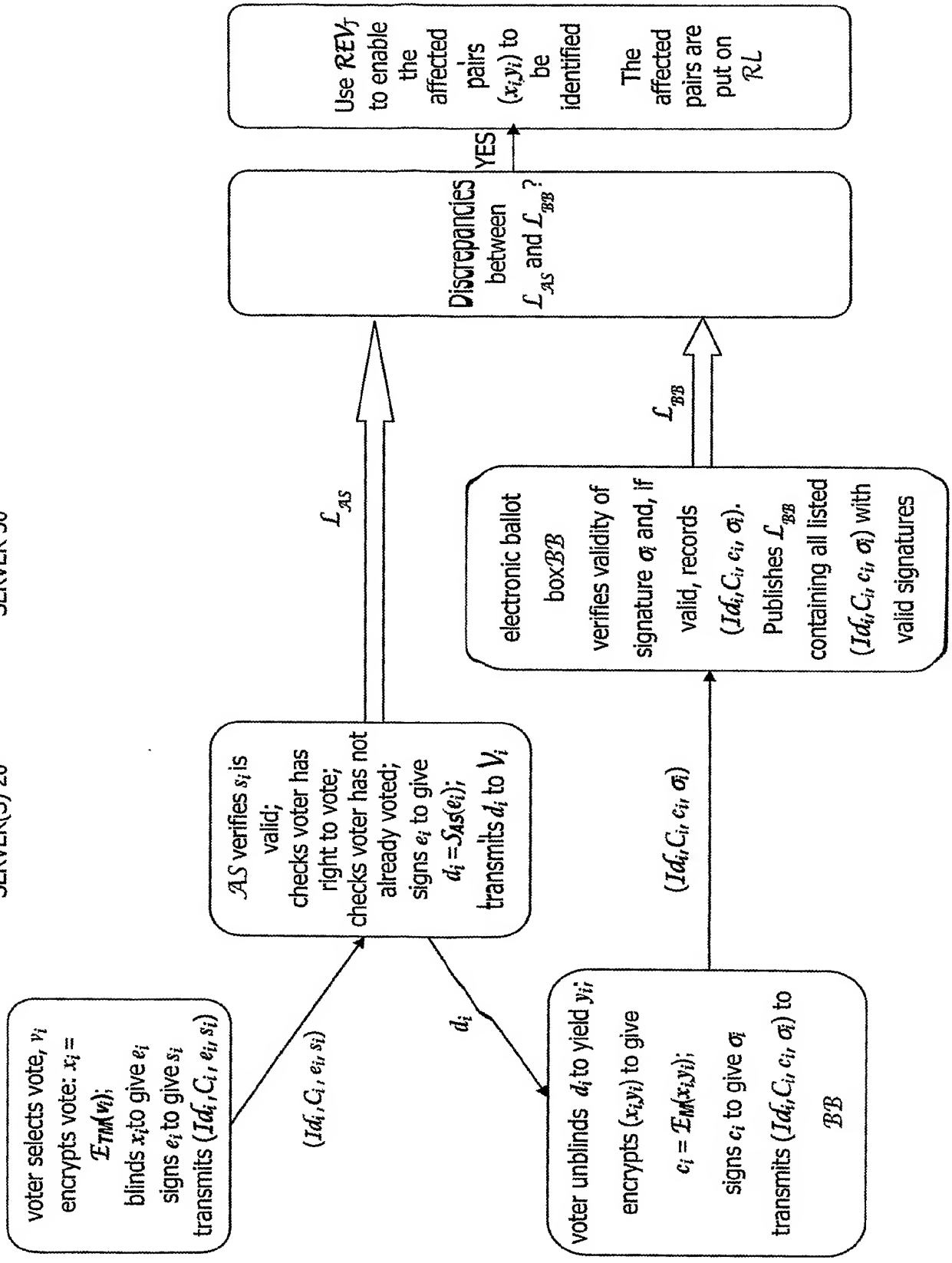

VOTER
ADMIN SERVER(S) 20
BULLETIN BOARD SERVER 30
voter selects vote, v_i
encrypts vote: $x_i = \mathcal{E}_{TM}(v_i)$;
blinds x_i to give e_i
signs e_i to give s_i
transmits (Id_i, C_i, e_i, s_i)
(Id_i, C_i, e_i, s_i)
$\mathcal{AS}$ verifies s_i is valid;
checks voter has right to vote;
checks voter has not already voted;
signs e_i to give $d_i = S_{AS}(e_i)$;
transmits d_i to V_i
$\mathcal{L}_{AS}$
Discrepancies between $\mathcal{L}_{AS}$ and $\mathcal{L}_{BB}$?
YES
Use REV_T to enable the affected pairs (x_i, y_i) to be identified
The affected pairs are put on RL
d_i
voter unblinds d_i to yield y_i;
encrypts (x_i, y_i) to give $c_i = \mathcal{E}_M(x_i, y_i)$;
signs c_i to give σ_i
transmits $(Id_i, C_i, c_i, \sigma_i)$ to $\mathcal{BB}$
$(Id_i, C_i, c_i, \sigma_i)$
electronic ballot box $\mathcal{BB}$
verifies validity of signature σ_i and, if valid, records $(Id_i, C_i, c_i, \sigma_i)$.
Publishes $\mathcal{L}_{BB}$ containing all listed $(Id_i, C_i, c_i, \sigma_i)$ with valid signatures
$\mathcal{L}_{BB}$

FIG.3

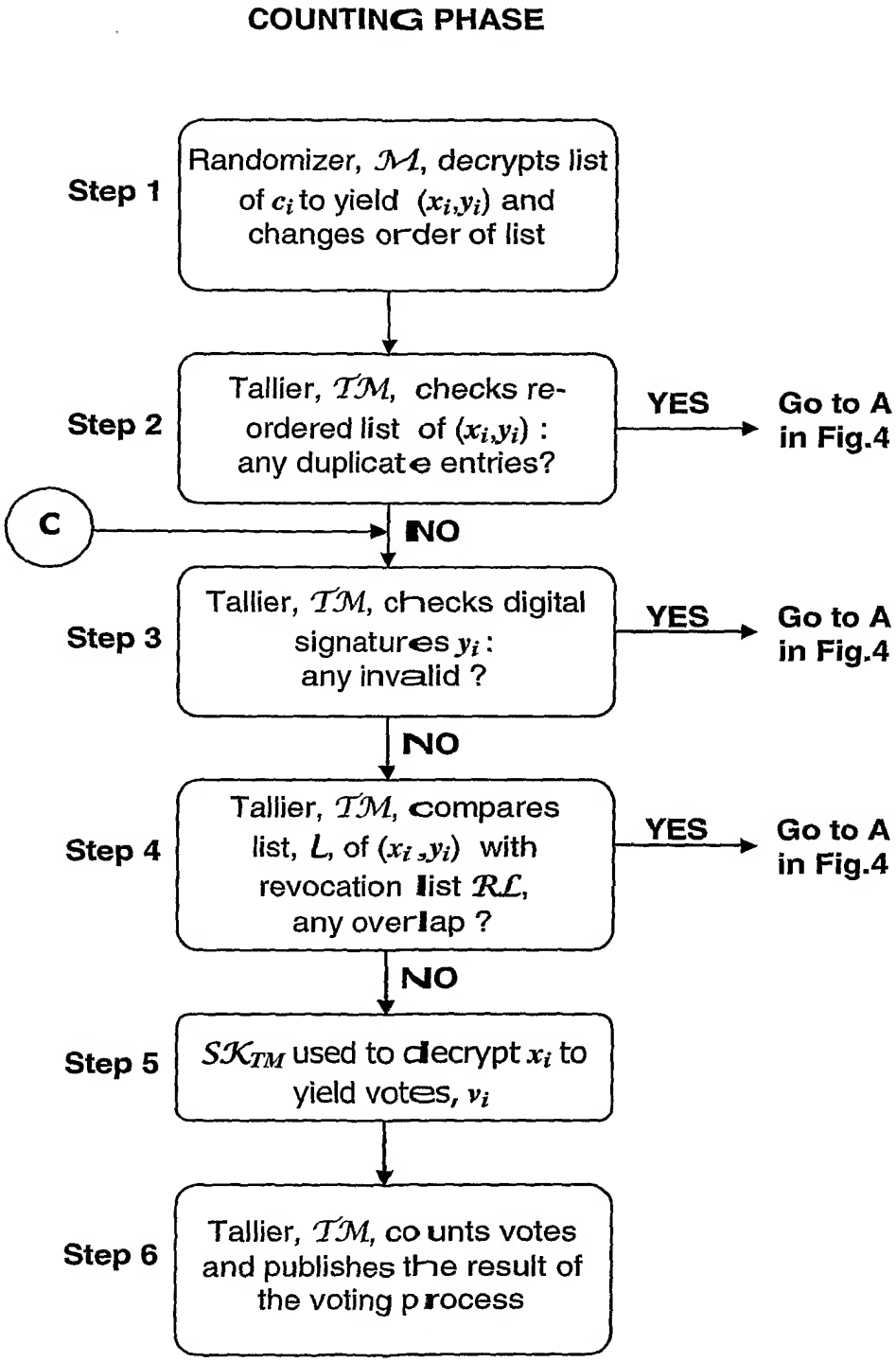

COUNTING PHASE
Step 1
Randomizer, $\mathcal{M}$, decrypts list of c_i to yield (x_i,y_i) and changes order of list
Step 2
Tallier, $\mathcal{TM}$, checks re-ordered list of (x_i,y_i) : any duplicate entries?
YES
Go to A in Fig.4
C
NO
Step 3
Tallier, $\mathcal{TM}$, checks digital signatures y_i : any invalid ?
YES
Go to A in Fig.4
NO
Step 4
Tallier, $\mathcal{TM}$, compares list, L, of (x_i,y_i) with revocation list $\mathcal{RL}$, any overlap ?
YES
Go to A in Fig.4
NO
Step 5
$\mathcal{SK}_{TM}$ used to decrypt x_i to yield votes, v_i
Step 6
Tallier, $\mathcal{TM}$, counts votes and publishes the result of the voting process

FIG.4

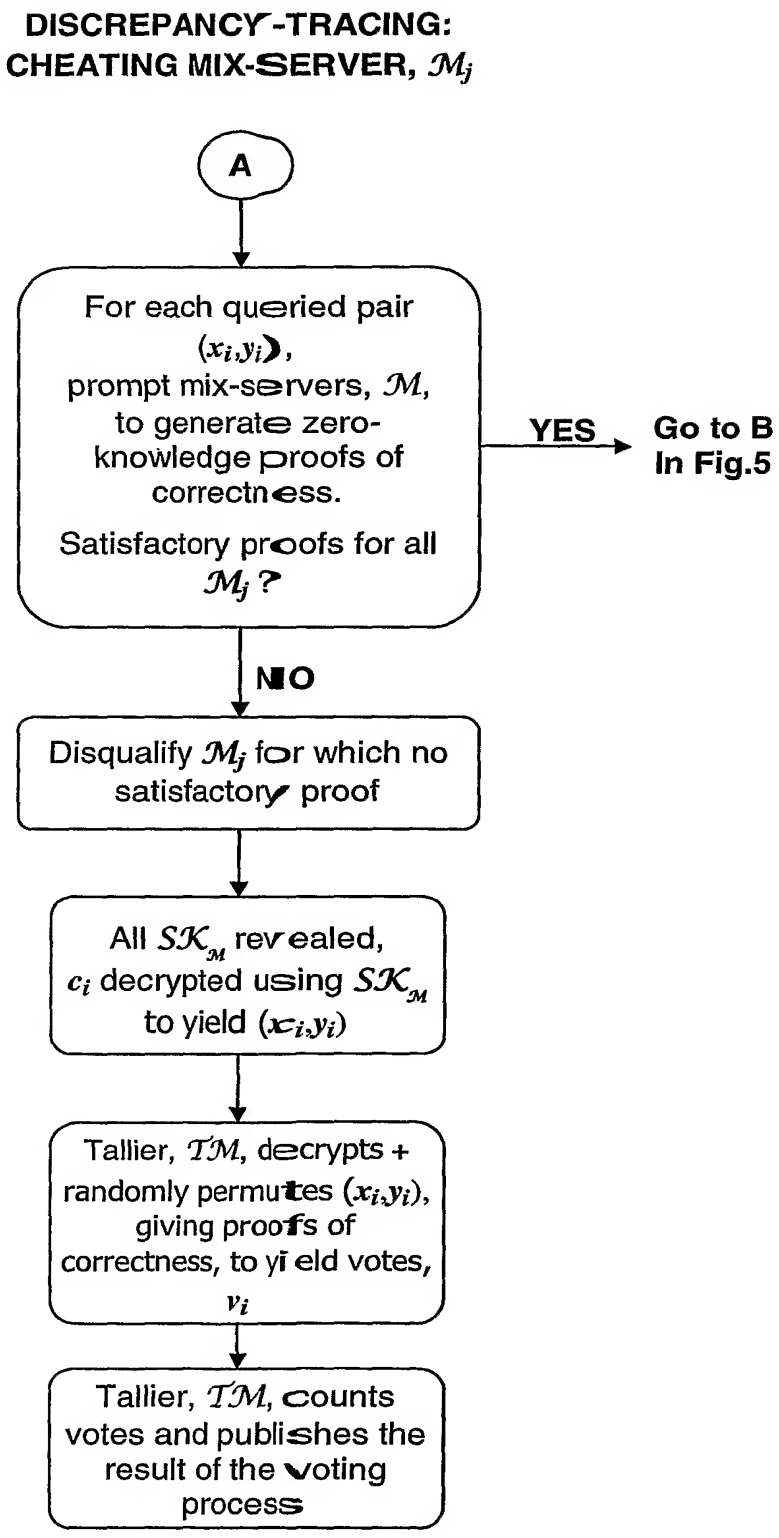
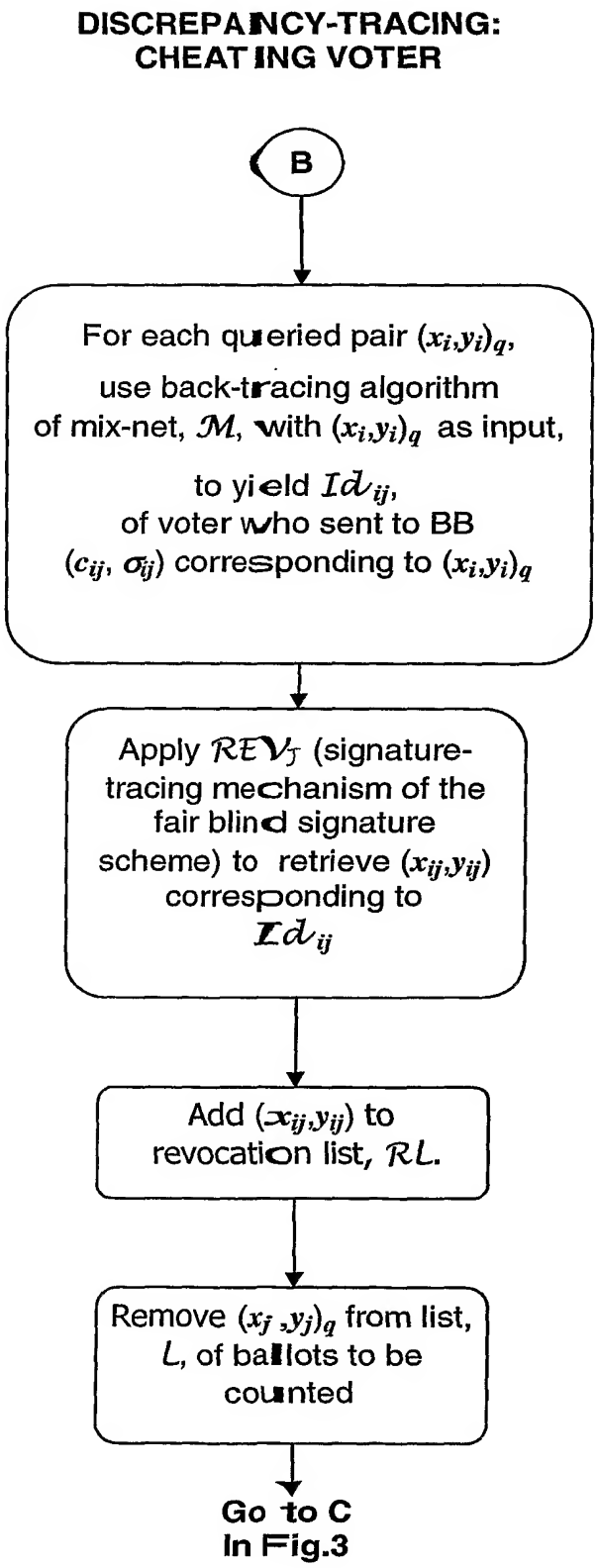

DISCREPANCY-TRACING:
CHEATING MIX-SERVER, $\mathcal{M}_j$
A
For each queried pair (x_i,y_i), prompt mix-servers, $\mathcal{M}$, to generate zero-knowledge proofs of correctness.
Satisfactory proofs for all $\mathcal{M}_j$?
YES
Go to B In Fig.5
NO
Disqualify $\mathcal{M}_j$ for which no satisfactory proof
All $\mathcal{SK}_{\mathcal{M}}$ revealed, c_i decrypted using $\mathcal{SK}_{\mathcal{M}}$ to yield (x_i,y_i)
Tallier, $\mathcal{TM}$, decrypts + randomly permutes (x_i,y_i), giving proofs of correctness, to yield votes, v_i
Tallier, $\mathcal{TM}$, counts votes and publishes the result of the voting process

FIG.5


DISCREPANCY-TRACING:
CHEATING VOTER
B
For each queried pair $(x_i,y_i)_q$, use back-tracing algorithm of mix-net, $\mathcal{M}$, with $(x_i,y_i)_q$ as input, to yield Id_{ij}, of voter who sent to BB (c_{ij}, σ_{ij}) corresponding to $(x_i,y_i)_q$
Apply $\mathcal{REV}_J$ (signature-tracing mechanism of the fair blind signature scheme) to retrieve (x_{ij},y_{ij}) corresponding to Id_{ij}
Add (x_{ij},y_{ij}) to revocation list, $\mathcal{RL}$.
Remove $(x_j,y_j)_q$ from list, L, of ballots to be counted
Go to C In Fig.3